

## AMENDMENTS TO THE CLAIMS

Please amend claim 20 and add claims 21-26 as follows:

- 1    1.    (Original) A method, comprising the computer-implemented steps of:  
2           determining a user identifier associated with a network device that has caused a security  
3           event in a network;  
4           causing the network device to receive a network address that is selected from a subset of  
5           addresses within a specified pool associated with suspected malicious network  
6           users; and  
7           configuring one or more security restrictions with respect to the selected network address.
- 1    2.    (Original) A method as recited in Claim 1, further comprising the steps of:  
2           receiving information identifying the security event in the network;  
3           correlating the security event information with network user information to result in  
4           determining the user identifier associated with the network device.
- 1    3.    (Original) A method as recited in Claim 1, wherein the network device uses dynamic host  
2           control protocol (DHCP) to obtain the network address, and wherein the step of causing  
3           the network device to receive a network address comprises resetting a port that is coupled  
4           to the network device to prompt a user to command the network device to request a new  
5           network address using DHCP.
- 1    4.    (Original) A method as recited in Claim 1, wherein the network device uses dynamic host  
2           control protocol (DHCP) to obtain the network address, and wherein the step of causing  
3           the network device to receive a network address comprises issuing a DHCP  
4           FORCE\_RENEW message to the network device.
- 1    5.    (Original) A method as recited in Claim 1, wherein the network device uses dynamic host  
2           control protocol (DHCP) to obtain the network address, and wherein the step of causing

3 the network device to receive a network address comprises prompting the network device  
4 to request a new network address using DHCP.

1 6. (Original) A method as recited in Claim 1, wherein the network device uses dynamic host  
2 control protocol (DHCP) to obtain the network address, and wherein the step of causing  
3 the network device to receive a network address comprises waiting for expiration of a  
4 lease for a current network address of the network device.

1 7. (Original) A method as recited in Claim 1, wherein the step of causing the network  
2 device to receive a network address comprises the step of providing the network device  
3 with an IP address that is selected from a plurality of IP addresses within a special IP  
4 subnet.

1 8. (Original) A method as recited in Claim 7, further comprising the step of publishing  
2 information describing characteristics of the special IP subnet to network service  
3 providers.

1 9. (Original) A method as recited in Claim 1, wherein the step of configuring security  
2 restrictions comprises the steps of modifying an internet protocol (IP) access control list  
3 (ACL) associated with a port that is coupled to the network device to permit entry of IP  
4 traffic from only the selected network address.

1 10. (Original) A method as recited in Claim 1, wherein the step of configuring security  
2 restrictions comprises the steps of modifying a media access control (MAC) ACL  
3 associated with a port that is coupled to the network device to permit entry of traffic only  
4 for a MAC address that is bound to the selected network address.

1 11. (Original) A method as recited in Claim 1, further comprising the steps of determining  
2 whether a malicious act caused the security event, and if so, providing information about  
3 the security event or malicious act to a security decision controller.

1 12. (Original) A method as recited in Claim 1, further comprising the steps of determining  
2 whether a malicious act caused the security event, and if not, removing the user from the  
3 elevated risk group.

1 13. (Original) A method as recited in Claim 1, further comprising the steps of determining  
2 whether a malicious act caused the security event, wherein a legal user action in the  
3 network is not determined to be a malicious act if the user is associated with a trusted  
4 customer of a network service provider.

1 14. (Original) A method, comprising the computer-implemented steps of:  
2 receiving information identifying a security event in a network;  
3 correlating the security event information with network user information to result in  
4 determining a network user associated with the network device.  
5 placing the user in an elevated risk security group;  
6 configuring one or more security restrictions with respect to the selected network address;  
7 determining whether a malicious act caused the security event;  
8 if a malicious act caused the security event, then providing information about the security  
9 event or malicious act to a security decision controller;  
10 if a malicious act did not cause the security event, then removing the user from the  
11 elevated risk group.

1 15. (Original) A method as recited in Claim 14, wherein placing the user identifier in an  
2 elevated risk security group further comprises the step of forcing the user to acquire a  
3 new network address from a specified group of network addresses that is reserved for  
4 users associated with elevated user risk;

1 16. (Original) A method as recited in Claim 15, wherein forcing the user to acquire a new  
2 network address comprises the steps of:

3 re-configuring a dynamic host control protocol (DHCP) server to require said server to  
4 issue any new network address to the network device only from a specified group  
5 of network addresses that is reserved for users associated with elevated user risk;  
6 performing any one of the steps of:

7 (a) resetting a port that is coupled to the network device to trigger the network device  
8 to request a new network address using DHCP;

9 (b) issuing a DHCP FORCE\_RENEW message to the network device;

10 (c) prompting the network device to request a new network address using DHCP;

11 (d) waiting for expiration of a lease for a current network address of the network  
12 device.

1 17. (Original) A method as recited in Claim 14, wherein the step of configuring one or more  
2 security restrictions comprises the steps of:

3 modifying an internet protocol (IP) access control list (ACL) associated with a port that is  
4 coupled to the network device to permit entry of IP traffic from only the selected  
5 network address;

6 modifying a media access control (MAC) ACL associated with the port to permit entry of  
7 traffic only for a MAC address that is bound to the selected network address.

1 18. (Original) A computer-readable medium carrying one or more sequences of instructions,  
2 which instructions, when executed by one or more processors, cause the one or more  
3 processors to carry out the steps of:

4 determining a user identifier associated with a network device that has caused a security  
5 event in a network;

6 causing the network device to receive a network address that is selected from a subset of  
7 addresses within a specified pool associated with suspected malicious network  
8 users; and

9 configuring one or more security restrictions with respect to the selected network address.

1 19. (Original) An apparatus, comprising:  
2 means for determining a user identifier associated with a network device that has caused  
3 a security event in a network;  
4 means for causing the network device to receive a network address that is selected from a  
5 subset of addresses within a specified pool associated with suspected malicious  
6 network users; and  
7 means for configuring one or more security restrictions with respect to the selected  
8 network address.

1 20. (Currently amended) An apparatus, comprising:  
2 a network interface that is coupled to the a data network for receiving one or more packet  
3 flows therefrom;  
4 a processor;  
5 one or more stored sequences of instructions which, when executed by the processor,  
6 cause the processor to carry out the steps of:  
7 determining a user identifier associated with a network device that has caused a security  
8 event in a network;  
9 causing the network device to receive a network address that is selected from a subset of  
10 addresses within a specified pool associated with suspected malicious network  
11 users; and  
12 configuring one or more security restrictions with respect to the selected network address.

1 21. (New) A computer-readable medium as recited in Claim 18, further comprising  
2 instructions for performing the steps as recited in any of Claims 2, 3, 4, 5, 6, 7, 8, 9, 10,  
3 11, 12, or 13.

1 22. (New) An apparatus as recited in Claim 19, further comprising means for performing the  
2 steps as recited in any of Claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, or 13.

1 23. (New) An apparatus as recited in Claim 20, further comprising instructions for  
2 performing the steps as recited in any of Claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, or 13.

1 24. (New) A computer-readable medium carrying one or more sequences of instructions,  
2 which instructions, when executed by one or more processors, cause the one or more  
3 processors to carry out the steps as recited in any of Claims 14, 15, 16, or 17.

1 25. (New) An apparatus comprising means for performing the functions recited in the steps  
2 of any of Claims 14, 15, 16, or 17.

1 26. (New) An apparatus, comprising:  
2 a network interface that is coupled to a data network for receiving one or more packet  
3 flows therefrom;  
4 a processor; and  
5 one or more stored sequences of instructions which, when executed by the processor,  
6 cause the processor to carry out the steps as recited in any of Claims 14, 15, 16, or  
7 17.